9110-9F

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2020-0051]

Privacy Act of 1974; System of Records

AGENCY: Science and Technology Directorate, U.S. Department of Homeland Security.

ACTION: Notice of a new system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the U.S. Department of Homeland Security (DHS) proposes to establish a new DHS system of records titled, "DHS/Science & Technology Directorate (S&T)-003 National Bioforensic Analysis Center Laboratory Elimination Database System of Records." This system of records describes DHS/S&T's collection, use, and maintenance of records on individuals who come into contact with or are in proximity to the National Bioforensic Analysis Center (NBFAC), a center within one of DHS's National Laboratories, or NBFAC biological samples or material. This newly established system will be included in DHS's inventory of record systems.

DATES: Submit comments on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. This new system will be effective upon publication. Routine uses will be effective **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by docket number DHS-2020-0051 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 202-343-4010.

- Mail: Lynn Parker Dupree, Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, D.C. 20528-0655.

Instructions: All submissions received must include the agency name and docket number DHS-2020-0051. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Maria Petrakis, (202) 254-7748, STPrivacy@hq.dhs.gov, S&T Privacy Officer, the Science and Technology Directorate, Mail Stop: 0205, U.S. Department of Homeland Security, 245 Murray Lane S.W., Washington, D.C. 20528. For privacy questions, please contact: Lynn Parker Dupree, (202) 343-1717, Privacy@hq.dhs.gov, Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, D.C. 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the U.S. Department of Homeland Security (DHS) Science & Technology Directorate (S&T) proposes to establish a new DHS system of records titled, "DHS/S&T-003 National Bioforensic Analysis Center Laboratory Elimination Database System of Records." The National Bioforensic Analysis Center (NBFAC) is a laboratory within one of DHS's National Laboratories, the National Biodefense Analysis and Countermeasures Center (NBACC). DHS/S&T and the Department of Justice (DOJ) Federal Bureau of Investigation Laboratory Division (FBI-LD) collaborate on NBACC operations and management, including NBFAC. DHS designated NBFAC to be the lead federal facility to conduct and facilitate the technical forensic analysis and interpretation of materials recovered

following a biological attack. NBFAC performs research, development, testing, and evaluation (RDT&E) activities to develop bioforensic capabilities and casework analysis in support of FBI law enforcement investigations requiring bioforensic analytic capabilities.

DHS/S&T uses the NBFAC Laboratory Elimination Database for contamination detection and prevention. The NBFAC Laboratory Elimination Database provides the capability to ensure that human deoxyribonucleic acid (DNA) sequences identified and reported in NBFAC's operational casework or RDT&E activities are not the result of accidental contamination by a person who has been in contact with or in proximity to NBFAC or its evidence, or RDT&E samples or biological material derived from the samples.

DHS/S&T establishes the database to collect, organize, store, maintain, and query information about laboratory-based or specimen-processing individuals to determine whether a contamination event may have occurred and which individual or individuals may be the source of an unintended contaminant present within a controlled environment, experiment, or scientific process. DHS/S&T also will use the database for contamination prevention purposes to identify, correct, and prevent the recurrence of the nonconformity that led to the contamination event. NBFAC compares individuals' information from the database to identify the possible source of a contaminant that may affect NBFAC's analytic results. NBFAC collects information from individuals, on a voluntary basis, who NBFAC has determined may be in a position to inadvertently contaminate samples or the biological materials derived from samples.

The database segregates data by core function and tracing function. Core function data consists of unique NBFAC-assigned identifiers and associated DNA. Tracing function data includes biographic information on the individual (e.g., name, institution, position, contact information, biological sex, or physical sample location), enabling

NBFAC to link core data to an individual, as needed, pursuant to NBFAC standard operating procedures.

DHS S&T creates this system of records in accordance with the authorities granted by 6 U.S.C. sec. 182 for conducting basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of DHS, through intramural and extramural programs. In addition, National Security Presidential Memorandum 14, Support for National Biodefense, and the National Biodefense Strategy serve as the primary authorities for the bioforensic work NBFAC performs in its laboratories. NBFAC uses the elimination database to ensure the accuracy of analytic results and improve laboratory procedures, as warranted, by evaluating and remediating any nonconformities that may have resulted in contamination.

NBFAC has taken steps to minimize the potential risks posed by the loss and/or unauthorized access, use, modification, destruction, or disclosure of individuals' information by adopting administrative, technical, and physical controls. NBFAC also takes steps to ensure the quality of the data NBFAC collects by collecting the information directly from the individual. The data S&T collects is the minimum relevant data needed for the contamination detection and prevention purposes of this system of records.

NBFAC limits access to the information by segregating the data into a core function and a tracing function. The core function is the data maintained and used to monitor and control for contamination purposes. NBFAC cannot identify an individual based on the core function data only. NBFAC would need the tracing function biographic information to be able to identify an individual, when necessary. NBFAC stores the tracing function data separately. For example, if a match is made between a DNA record from the core function data and a suspected contaminant, if needed, NBFAC may retrieve additional information on the individual (e.g., name, institution, position, contact information, biological sex, or physical sample location) from a separate tracing function

area in the database, in accordance with NBFAC the database standard operating procedure.

Consistent with DHS's information sharing mission, information stored in the DHS/S&T-003 National Bioforensic Analysis Center Laboratory Elimination Database System of Records may be shared with other DHS Components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, DHS/S&T may share information with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice. This newly established system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which Federal Government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Additionally, the Judicial Redress Act (JRA) provides covered persons with a statutory right to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

Below is the description of the DHS/S&T-003 National Bioforensic Analysis Center Laboratory Elimination Database System of Records.

In accordance with 5 U.S.C. sec. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

SYSTEM NAME AND NUMBER: U.S. Department of Homeland Security (DHS)/Science & Technology Directorate (S&T)-003 National Bioforensic Analysis Center Laboratory Elimination Database System of Records.

SECURITY CLASSIFICATION: Unclassified and Classified.

SYSTEM LOCATION: Records are maintained at NBFAC within NBACC at Ft. Detrick, MD.

SYSTEM MANAGER(S): Director, Office of National Laboratories, Science & Technology Directorate, U.S. Department of Homeland Security, Room #10-027, S&T Division, Mail Stop: 0205, 245 Murray Lane S.W., Washington, D.C. 20528-0205, (202)-254-8227.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: The Homeland Security Act of 2002, Public Law 107-296, Sec. 302 (codified at 6 U.S.C. sec. 182); National Security Presidential Memorandum 14, Support for National Biodefense, and the National Biodefense Strategy; the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638, sec. 8306 (Dec. 2004), 6 U.S.C. sec. 112 note, 6 CFR Part 46, and 42 U.S.C. sec. 300v-1, and 45 CFR Part 46, Subpart A, to the extent an activity meets the definition of research on human subjects.

PURPOSE(S) OF THE SYSTEM: The purpose of this system is to determine whether a contamination event may have occurred related to NBFAC's operational casework or RDT&E activities; and if so, which individual or individuals may be the source of an unintended contaminant present within a controlled environment, experiment, or scientific process, and to prevent the recurrence of the nonconformity that led to contamination event.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: NBFAC personnel and non-NBFAC personnel that have access to the laboratory, including maintenance, instrument service personnel and visitors, and non-NBFAC personnel that may have had contact with items prior to the commencement of the controlled activities.

The NBFAC individuals include: (1) NBFAC evidence handlers, chain of custody staff, technicians, principal investigators, engineers, safety staff, security staff, maintenance staff, and internal auditors that handle evidence items, or biological material derived from evidence items, or access DNA-sensitive NBFAC laboratories; and (2) FBI staff that handle evidence items, or biological material derived from evidence items, or access DNA-sensitive NBFAC laboratories.

Individuals external to NBFAC include non-NBFAC personnel who are evidence collectors and handlers and casework technicians who handle evidence or derived biological materials prior to their arrival at NBFAC, engineers and technicians that access DNA-sensitive NBFAC laboratories to install or maintain equipment, auditors/inspectors that access DNA-sensitive NBFAC laboratories, and visitors granted access to DNA-sensitive NBFAC laboratories.

CATEGORIES OF RECORDS IN THE SYSTEM:

- Individual's full name;
- Unique NBFAC identifier for the individual;
- An external partner's personal identifier for information about an individual, other than a name, (e.g., employee identification number or badge number);
- Institutional or organizational affiliation;
- Institutional or organizational position;
- Contact information including, phone numbers, email addresses, physical addresses;
- Individual's biological sex;

- Individual's collected DNA sample and the sample's physical location information (stored and maintained in the database); and
- Individual's DNA sequence data, but not the full genome sequence.

RECORD SOURCE CATEGORIES: Records are obtained from NBFAC and non-NBFAC personnel. External partner agencies may provide information about their personnel who have been in contact or proximity to NBFAC DNA-sensitive laboratories or its biological samples or material.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. sec. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. sec. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including the U.S. Attorneys Offices, or other federal agencies conducting litigation or proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;

2. Any employee or former employee of DHS in his/her official capacity;

3. Any employee or former employee of DHS in his/her individual capacity, only when DOJ or DHS has agreed to represent the employee; or

4. The United States or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. secs. 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when (1) DHS suspects or has confirmed that there has been a breach of the system of records; (2) DHS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DHS (including its information systems, programs, and operations), the federal government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

F. To another federal agency or federal entity, when DHS determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

G. To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

I. To a federal agency for a statistical or research purpose, including the development of methods or resources to support statistical or research activities, provided that the records support DHS programs and activities that relate to the purpose(s) stated in this SORN, and will not be used in whole or in part in making any determination regarding an individual's rights, benefits, or privileges under federal programs, or published in any manner that identifies an individual.

J. To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, when 1) the NBACC has entered into an agreement with such agency to process samples on behalf of the agency, 2) either NBACC or the partner agency has reason to believe a contamination event has occurred, and 3) the partner agency demonstrates to NBACC that the contamination event relates to or affects a law enforcement investigation, and 4) NBACC determines that release of the records would assist in identifying and resolving a contamination event.

K. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations, with the approval of the Chief Privacy Officer, when DHS is aware of a need to use relevant data, that relate to the purpose(s) stated in this SORN, for purposes of testing new technology.

L. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute a clearly unwarranted invasion of personal privacy.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: DHS/S&T typically stores records in this system electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, and digital media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: DHS/S&T may retrieve records by name, NBFAC identifier, or other personal identifier.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: DHS/S&T has proposed a records retention schedule to NARA. DHS/S&T proposes a 20-year retention period for (1) records generated for use in law enforcement cases, with the potential for appeal; and (2) records in research and development files or projects, not used in law enforcement cases, to allow time to evaluate their historic significance.

In some instances, DHS/S&T seeks permanent retention for records in significant law enforcement cases or projects involving novel or complex issues, public interest, media attention, or congressional scrutiny and a five-year retention period for records that document compliance with International Organization for Standardization (ISO) 17025 requirements to carry out tests and/or calibrations, including sampling.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DHS/S&T safeguards records in this system according to applicable rules and policies, including all

applicable DHS automated systems security and access policies. DHS/S&T has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RECORD ACCESS PROCEDURES: Individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Component Privacy Officer or Component Freedom of Information Act Officer, whose contact information can be found at http://www.dhs.gov/foia under "Contact Information." If an individual believes more than one component maintains Privacy Act records concerning him or her, or if the request is for records maintained at a DHS Headquarters office, the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, U.S. Department of Homeland Security, Washington, D.C. 20528-0655, or electronically at https://www.dhs.gov/dhs-foia-privacy-act-request-submission-form. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, certain records about you may be available under the Freedom of Information Act.

When an individual is seeking records about himself or herself from this system of records or any other Departmental system of records, the individual's request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. The individual must first verify his/her identity, meaning that the individual must provide his/her full name, current address, and date and place of birth. The individual must sign the request, and the individual's signature must either be notarized or submitted under 28 U.S.C. sec. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. An individual may obtain more information about this process at http://www.dhs.gov/foia. In addition, the individual should, whenever possible:

- Describe the records sought, including any circumstances or reasons why the Department would have information being requested;
- Identify which component(s) of the Department or Department Headquarters Office he or she believes may have the information;
- Specify the timeline when the individual believes the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS Headquarters Office or component agency may have responsive records;

If the request is seeking records pertaining to another living individual, the request must include a statement from the living individual verifying the identity of the individual, as described in the verification steps above, and provide a statement from the living individual certifying the individual's agreement that records concerning the individual may be released to you.

Without the above information, the component(s) may not be able to conduct an effective search, and the individual's request may be denied due to lack of specificity or lack of compliance with applicable regulations.

CONTESTING RECORD PROCEDURES: For records covered by the Privacy Act or covered JRA records, individuals may make a request for amendment or correction of a record of the Department about the individual by writing directly to the Department component that maintains the record, unless the record is not subject to amendment or correction. The request should identify each particular record in question, state the amendment or correction desired, and state why the individual believes that the record is not accurate, relevant, timely, or complete. The individual may submit any documentation that would be helpful. If the individual believes that the same record is in more than one system of records, the request should state that and be addressed to each component that maintains a system of records containing the record. Even if neither the

Privacy Act nor the Judicial Redress Act provide a right of access, individuals may seek to amend records following the "access procedures" above. DHS/S&T, in its discretion, may choose to make the requested amendment. However, neither this system of records notice, nor DHS/S&T's making a requested amendment, confers to individuals any right to access, contest, or amend records not covered by the Privacy Act or Judicial Redress Act.

NOTIFICATION PROCEDURES: See "Record Access Procedures" above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None. When this system receives a record from another system exempted in that source system under 5 U.S.C. sec. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated.

HISTORY: N/A.

*****

Lynn Parker Dupree,

Chief Privacy Officer,

U.S. Department of Homeland Security.

[FR Doc. 2021-09937 Filed: 5/10/2021 8:45 am; Publication Date: 5/11/2021]